APLIKASI MATRIKS INVERS TERGENERALISASI PADA DIFFIE-HELLMAN (DH)

TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Sains pada
Jurusan Matematika

Oleh:

MIA FADILLA
10854004415

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU

2012

APLIKASI MATRIKS INVERS TERGENERALISASI PADA DIFFIE-HELLMAN (DH)

MIA FADILLA
10854004415

Tanggal Sidang : 27 Juni 2012
Tanggal Wisuda : November 2012

Jurusan Matematika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. HR. Soebrantas No.155 Pekanbaru

ABSTRAK

Diffie-Hellman merupakan algoritma pertukaran kunci. Kunci pada Algoritma Diffie-Hellman berbentuk bilangan yang sangat besar. Untuk perluasan pembentukan kunci maka bilangan yang sangat besar pada algoritma Diffie-Hellman diganti dengan menggunakan matriks, dengan alasan pada proses pembentukan sebuah pesan menjadi tidak dapat dibaca umumnya dilakukan dengan menggunakan kunci berupa matriks. Selanjutnya matriks invers tergeneralisasi memiliki hal yang unik untuk diaplikasikan pada proses pertukaran kunci dengan menggunakan algoritma Diffie-Hellman. Ide awal matriks invers tergeneralisasi yaitu invers pada matriks biasanya memenuhi ketentuan yaitu non-singular atau matriks yang mempunyai $det \neq 0$. Namun faktanya tidak semua matriks mempunyai $det \neq 0$. Untuk mencari nilai invers pada matriks singular maka terciptalah ide mengenai invers matriks secara umum yang dikenal dengan matriks invers tergeneralisasi. Kunci yang dihasilkan berupa sebuah matriks yang telah dioperasikan pada langkah-langkah yang ada pada algoritma Diffie-Hellman. Jika perhitungan benar maka kunci yang dihasilkan pada pertukaran akan sama.

Katakunci: Algoritma Diffie-Hellman (DH), Matriks singular, Matriks Invers Tergeneralisasi.

KATA PENGANTAR

Alhamdulillahirabbil'alamin, puji syukur penulis ucapkan kehadirat Allah SWT. atas segala limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas akhir dengan judul **"APLIKASI MATRIKS INVERS TERGENERALISASI PADA DIFFIE-HELLMAN"**. Shalawat beriring salam tak lupa penulis hantarkan pada nabi Muhammad SAW, karena dengan perjuangan dari beliaulah penulis dapat merasakan kehidupan yang begitu indah dimasa sekarang ini. Penulisan Tugas akhir ini dimaksudkan untuk memenuhi salah satu syarat dalam rangka menyelesaikan studi Strata 1 (S1) di UIN Suska Riau.

Penyusunan dan penyelesaian tugas akhir ini, penulis tidak terlepas dari bantuan berbagai pihak, baik langsung maupun tidak langsung. Untuk itu penulis mengucapkan terimakasih yang tak terhingga kepada kedua orang tua tercinta ayahanda dan ibunda yang tidak pernah lelah dalam mencurahkan kasih sayang, perhatian, do'a, dan dukungan untuk menyelesaikan tugas akhir ini. Selanjutnya ucapan terimakasih kepada :

1. Bapak Prof. Dr. H. M. Nazir selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Ibu Dra. Hj. Yenita Morena, M.Si selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Ibu Sri Basriati, M.Sc selaku Ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
4. Ibu Yuslenita Muda, M.Sc selaku pembimbing yang telah banyak membantu, mengarahkan, mendukung, dan membimbing penulis dengan penuh kesabarannya dalam penulisan Tugas akhir ini.
5. Ibu Fitri Aryani, M.Sc selaku penguji I dan Koordinator TA yang telah banyak membantu, memberikan kritikan dan saran serta dukungan dalam penulisan tugas akhir ini.

6. Ibu Sri Basriati, M.Sc selaku penguji II yang telah banyak membantu dan memberikan kritikan serta saran dalam penulisan tugas akhir ini.
7. Semua dosen-dosen Jurusan Matematika yang telah memberikan dukungan serta saran dalam menyelesaikan tugas akhir ini.

Penulis telah berusaha semaksimal mungkin dalam penyusunan tugas akhir ini. Walaupun demikian tidak tertutup kemungkinan adanya kesalahan dan kekurangan baik dalam penulisan maupun dalam penyajian materi. Penulis mengharapkan kritik dan saran dari berbagai pihak demi kesempurnaan tugas akhir ini.

Pekanbaru, 27 Juni 2012

Mia Fadilla

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan dan keaslian data adalah hal yang penting dalam proses pengiriman data dari seorang pengirim pesan ke penerimanya. Pengirim harus yakin bahwa pesan yang dikirim tersebut utuh, tidak dibaca orang lain, tidak dimodifikasi, dan sampai kepada orang yang tepat. Penerima pesan juga harus yakin bahwa pesan yang diterima tersebut benar, masih asli tanpa modifikasi orang lain. Agar masalah tersebut terpecahkan, maka muncullah ilmu penyandian yang dikenal dengan Kriptografi.

Secara umum Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti keabsahan, integritas data, serta autentifikasi data.

Sejarahnya, kriptografi mulai berkembang pada tahun 400 SM. Kemudian Kriptografi berkembang lebih baik sehingga pada tahun 1976, Whitfield Diffie dan Martin Hellman memperkenalkan teknik kriptografi, yang sekarang populer disebut sistem kunci publik, bahwa media transmisi (umum) dapat digunakan untuk mentransmisikan informasi-informasi yang bersifat rahasia. Algoritma Diffie-Hellman (DH) hanya dapat digunakan untuk pertukaran kunci (simetris) dan tidak dapat digunakan untuk enskripsi/ deskripsi maupun untuk tanda tangan digital (Yusuf Kurniawan, 2004).

Algoritma Diffie-Hellman pada dasarnya menggunakan teori bilangan yang sangat besar pada pertukaran kuncinya. Namun pada umumnya proses pembentukan sebuah pesan menjadi tidak dapat dibaca menggunakan kunci (*key*) berupa matriks, maka untuk pengembangan penggunaan algoritma Diffie-Hellman bilangan yang sangat besar tersebut diganti dengan matriks. Sementara itu, matriks invers tergeneralisasi memiliki hal yang unik untuk diaplikasikan pada proses pertukaran kunci dengan menggunakan algoritma Diffie-Hellman.

Berdasarkan latar belakang di atas maka diketahui belum ada peneliti yang menggunakan matriks invers tergeneralisasi pada algoritma Diffie-Hellman.

Sehingga pada tugas akhir ini penulis melakukan penelitian dengan judul "**Aplikasi Matriks Invers Tergeneralisasi pada Diffie-Hellman"**.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini yaitu bagaimana mengaplikasikan matriks invers tergeneralisasi pada Algoritma Diffie-Hellman ?

1.3 Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah mendapatkan solusi berupa kunci yang diperoleh dari Algoritma Diffie-Hellman dengan mengaplikasikan matriks invers tergeneralisasi.

1.4 Batasan Masalah

Berdasarkan rumusan masalah, maka harus dilakukan batasan masalah agar tujuan dari penelitian ini dapat dicapai dengan baik dan tepat pada sasarannya. Permasalahan pada penelitian ini dibatasi pada hal-hal sebagai berikut :

1. Matriks Invers Tergeneralisasi dibatasi hanya matriks persegi (matriks kuadarat) singular.
2. Aritmatika Modulo dibatasi hanya menggunakan operator $mod\ 29$.
3. Algoritma Diffie-Hellman dibatasi hanya merancang sebuah kunci.

1.5 Manfaat Penulisan

Adapun manfaat yang bisa diperoleh dari penelitian ini adalah:

1. Memberikan wawasan baru bagi penulis dan pembaca tentang aplikasi aljabar berupa pemecahan sandi dengan menggunakan matriks.
2. Penulis dapat mengetahui dan menentukan kunci atau kode yang terbaik dari proses pertukaran kunci dengan menggunakan algoritma Diffie-Hellman tersebut.
3. Memberikan informasi kepada pembaca tentang cara-cara atau langkah-langkah pembentukan kunci atau kode.

4. Menambah pemahaman tentang konsep matriks invers tergeneralisasi secara umum.
5. Memberikan informasi kepada pembaca tentang aplikasi matriks invers tergeneralisasi pada kriptografi.

1.6 Sistematika Penulisan

Dalam penulisan skripsi ini, penulis menggunakan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Bab ini mencakup mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang teori-teori yang mendukung dalam menyelesaikan bagian pembahasan masalah. Teori-teori tersebut antara lain meliputi Matriks Invers Tergeneralisasi, Kriptografi, algoritma Diffie-Hellman dan Aplikasi Matriks Invers Tergeneralisasi pada Diffie-Hellman.

BAB III METODOLOGI PENELITIAN

Bab ini berisi prosedur atau langkah-langkah untuk mendapatkan hasil pembentukan kunci dengan mengguanakan matriks invers tergeneralisasi.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini berisikan tentang pembahasan penelitian yang didukung dengan literatur yang telah ada.

BAB V PENUTUP

Bab ini berisikan tentang kesimpulan dari seluruh pembahasan pada bab-bab sebelumnya dan saran yang berkaitan dengan kajian ini.

BAB II
LANDASAN TEORI

2.1 Determinan

Pengertian determinan matriks adalah jumlah semua hasil perkalian elementer yang bertanda dari A. Determinan dari matriks bujur sangkar $A = [a_{ij}]_{n\times n}$ bernilai skalar. Determinan dinotasikan dengan $\det A$ atau $|A|$. Beberapa metode untuk menghitung determinan matriks seperti sirus, kofaktor, adjoin dan lain-lain.

Teorema 2.1 (Anton, Howard. 1998) Misalkan A adalah suatu matriks bujur sangkar, maka berlaku :

1. Jika $|A| = 0$ maka A disebut matriks singular. Matriks singular tidak mempunyai invers.
2. Jika$|A| \neq 0$ maka A disebut matriks non-singular. Matriks non-singular mempunyai invers.
3. Jika semua elemen baris A adalah nol, maka$|A| = 0$.
4. $|A| = |A^T|$.

Bukti :

1. Diketahui matriks A berukuran $n \times n$. Akan ditunjukkan $|A| = 0$ atau dengan kata lain akan ditunjukkan matriks A adalah matriks singular.

   Diambil sebarang nilai a_{ij} pada matriks A berukuran $n \times n$ dimana $a_{ij} \in \mathbb{R}$ sehingga $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dengan $\det A = (ad - bc) = 0$, maka matriks tersebut tunggal dan tidak mempunyai kebalikan. Dari defenisi diketahui bahwa determinan adalah perkalian dari elemen matriks, jika terdapat nilai elemen matriks yang identik antara baris satu dengan baris yang lain maka matriks A pasti memiliki $|A| = 0$. Pembuktian ini juga dapat dilihat pada metode untuk mendapatkan invers (kebalikan) yaitu metode adjoin, dimana $A^{-1} = \frac{1}{det(A)} Adj\ A$, jika $\det(A) = 0$ maka matriks A jelas tidak mempunyai invers.

■

2. Diketahui matriks A berukuran $n \times n$. Akan ditunjukkan $|A| \neq 0$ atau dengan kata lain akan ditunjukkan matriks A adalah matriks non-singular.

   Diambil sebarang nilai a_{ij} pada matriks A berukuran $n \times n$ dimana $a_{ij} \in \mathbb{R}$ sehingga $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$dengan $\det A = (ad - bc) \neq 0$, Pembuktian ini dapat dilihat pada metode untuk mencari invers yaitu metode adjoin, dimana $A^{-1} = \frac{1}{det(A)} Adj\ A$, jika $\det(A) \neq 0$ maka matriks A mempunyai invers dan terbukti bahwa matriks A non-singular. ■

3. Diketahui semua elemen baris matriks A adalah nol. Akan ditunjukkan $|A| = 0$.

   Karena diketahui semua elemen baris matriks A adalah nol maka ambil nilai $a_{ij} = 0$ pada matriks A berukuran $n \times n$ sehingga $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\det A = 0 - 0 = 0$. ■

4. Diketahui Diketahui matriks A berukuran $n \times n$. Akan ditunjukkan $|A| = |A^T|$.

   Nilai determinan tidak berubah bila semua baris diubah menjadi kolom begitu juga sebaliknya.

   Teorema ini juga akan dibuktikan dengan contoh berikut.

   Contoh 2.1

   Diberikan matriks$\begin{bmatrix} 3 & 1 \\ 5 & 7 \end{bmatrix}$, tunjukkan$|A| = |A^T|$!

   Penyelesaian :

   $|A| = \begin{vmatrix} 3 & 1 \\ 5 & 7 \end{vmatrix} = (21 - 5) = 16$

   $|A^T| = \begin{vmatrix} 3 & 5 \\ 1 & 7 \end{vmatrix} = (21 - 5) = 16$

   $|A| = |A^T| = 16 = 16.$ ■

Teorema 2.2 (Anton, Howard. 1998) Sebuah matriks A kuadrat dapat dibalik jika dan hanya jika $\det A \neq 0$.

Bukti :

Diketahui matriks A kuadrat. Akan ditunjukkan matriks A dapat dibalik jika dan hanya jika $\det A \neq 0$.

Defenisi dari kebalikan adalah jika $AB = BA = I$, maka A dapat dibalik.

→ Misalkan $AB = C$ maka $C = I$ sehingga $\det C = I$, artinya $\det C \neq 0$ karena hasil dari $\det C$ adalah identitas. Hal ini berarti $\det A$ juga tidak sama dengan nol. ■

← Misalkan $\det A \neq 0$ maka $\det C \neq 0$, sehingga A dapat dibalik karena $C = AB = BA = I$.

Teorema di atas juga dapat dibuktikan dengan contoh berikut :

Contoh 2.2 :

Diberikan matriks $P = \begin{bmatrix} -2 & 2 & -3 \\ -1 & 1 & 3 \\ 2 & 0 & -1 \end{bmatrix}$.

Carilah determinan dari matriks P !

Penyelesaian:

Dengan menggunakan metode sarrus

$$\begin{bmatrix} -2 & 2 & -3 & -2 & 2 \\ -1 & 1 & 3 & -1 & 1 \\ 2 & 0 & -1 & 2 & 0 \end{bmatrix}$$

$= \big[\big((-2)(1)(-1)\big) + \big((2)(3)(2)\big) + \big((-3)(-1)(0)\big)\big]$

$\quad -\big[\big((2)(-1)(-1)\big) + \quad \big((-2)(3)(0)\big) + \big((-3)(1)(2)\big)\big]$

$= [2 + 12 + 0] - [2 + 0 + (-6)]$

$= 14 + 4 = 18.$

2.2 Invers

Defenisi 2.1 (Anton, Howard. 1998) Misal A adalah matriks kuadrat, jika dapat dicari matriks B sehingga $AB = BA = I$, maka A dikatakan dapat dibalik (*invertible*) dan B dinamakan invers dari A.

Teorema 2.3 (Anton, Howard. 1998) Jika B dan C adalah invers matrik A, maka $B = C$.

Bukti :

Diketahui B dan C adalah invers matriks A. Akan ditunjukkan bahwa $B = C$.

Karena B invers matrik A berarti $AB = BA = I$, dan karena C invers matrik A berarti $AC = CA = I$. kemudian kalikan kedua ruas dengan C pada $BA = I$ diperoleh $(BA)C = IC = C$. Untuk $AC = I$ kalikan kedua ruas dengan B diperoleh $(BA)C = B(AC) = BI = B$, sehingga $C = B$ atau $B = C$. ∎

Teorema 2.4 (Anton, Howard. 1998) Jika A dan B adalah matriks-matriks yang dapat dibalik dan ukuran-ukurannya sama, maka $(AB)^{-1} = B^{-1}A^{-1}$.

Bukti :

Diketahui A dan B adalah matriks-matriks yang dapat dibalik dan berukuran sama. Akan ditunjukkan $(AB)^{-1} = B^{-1}A^{-1}$.

Jika dapat ditunjukkan bahwa $(AB)(B^{-1}A^{-1}) = (B^{-1}A^{-1})(AB) = I$, maka AB adalah matriks yang dapat dibalik sehingga $(AB)(B^{-1}A^{-1}) = I$ jika dikalikan kedua ruas dengan$(AB)^{-1}$diperoleh $(AB)^{-1}(AB)(B^{-1}A^{-1}) = (AB)^{-1}I$

$I(B^{-1}A^{-1}) = (AB)^{-1}$atau $(AB)^{-1} = B^{-1}A^{-1}$. ∎

Teorema 2.5 (Anton, Howard. 1998) Misalkan A dan B adalah suatu matriks bujur sangkar, maka berlaku :

1. $(AB)^{-1} = B^{-1}A^{-1}$.
2. $(A^{-1})^T = (A^T)^{-1}$.

Bukti :

1. Bukti teorema ini sama dengan bukti pada teorema 2.4**.**
2. Diketahui A dan B adalah matriks bujur sangkar. Akan ditunjukkan bahwa $(A^{-1})^T = (A^T)^{-1}$.

   Dengan menggunaka defenisi invers, yaitu dengan matriks invertibel diperoleh $A^T(A^{-1})^T = (A^{-1})^T A^T = I$

   Diketahui bahwa $I^T = I$, maka diperoleh :

   $A^T(A^{-1})^T = (A^{-1}A)^T = I^T = I$

   $(A^{-1})^T A^T = (AA^{-1})^T = I^T = I$. ∎

Contoh 2.3 :

Diberikan matriks $A = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$

Carilah invers dari matriks A !

Penyelesaian :

Misalkan $A^{-1} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ maka berlaku $\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Bila dikalikan : $\begin{bmatrix} 2a_1 + a_3 & 2a_2 + a_4 \\ 4a_1 + 3a_3 & 4a_2 + 3a_4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ maka diselesaikan

$2a_1 + a_3 = 1$, $2a_2 + a_4 = 0$, $4a_1 + 3a_3 = 0$ dan $4a_2 + 3a_4$ maka dengan eliminasi diperoleh : $a_1 = \frac{3}{2}$, $a_2 = -\frac{1}{2}$, $a_3 = -2$, dan $a_4 = 1$.

Jadi $A^{-1} = \begin{bmatrix} \frac{3}{2} & -\frac{1}{2} \\ -2 & 1 \end{bmatrix}$

Atau menggunakan matriks adjoin dengan cara :

$A = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$

$Adj\ A = \begin{bmatrix} 3 & -1 \\ -4 & 2 \end{bmatrix}$, $\det A = 2$

Jadi $A^{-1} = \frac{\begin{bmatrix} 3 & -1 \\ -4 & 2 \end{bmatrix}}{2} = \begin{bmatrix} \frac{3}{2} & -\frac{1}{2} \\ -2 & 1 \end{bmatrix}$.

2.3 Matriks Invers Tergeneralisasi

Ide awal dari invers matriks tergeneralisasi (*Generalized Inverses of Matrix*) adalah untuk menggeneralisasi pengertian invers matriks. Jika A adalah matriks invertibel, maka terdapat matriks G sedemikian sehingga berlaku $AG = GA = I$ dengan I adalah matriks identitas. Dalam hal ini G disebut matriks invers dari A, dinotasikan dengan A^{-1}.

Langkah-langkah untuk mendapatkan matriks invers tergeneralisasi seperti yang diambil dalam jurnal *On The Generalisized Inverse of a Matrikx* (Adetunde dkk, 2010) :

a. Diketahui rank r pada matriks A yang mencerminkan matriks non-singular, kemudian diambil submatriks dari matriks A disebut dengan matriks M.

b. Invers matriks M, kemudian tansposkan.

c. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks M diambil dari matriks A.

d. Mengganti semua elemen lain dengan nol.

e. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi.

Jika G adalah invers matrik tergeneralisasi dari A maka :

a. $AGA = A$.

b. G tidak unik.

c. Matriks G berukuran tidak sama dengan matriks A.

Sifat-sifat umum matriks invers tergeneralisasi :

a. $GAG = G$.

b. $AGA = A$.

Contoh 2.4 :

Diberikan matriks $A = \begin{bmatrix} 4 & 1 & 3 \\ 1 & 1 & 1 \\ 2 & 5 & 3 \end{bmatrix}$.

Carilah invers tergeneralisasi matriks A !

Penyelesaian :

Terlebih dahulu dilakukan pencarian rank matriks A agar diketahui ordo matriks M pada langkah selanjutnya. Rank akan dicari dengan menggunakan OBE, berikut perhitungannya :

$$\begin{bmatrix} 4 & 1 & 3 \\ 1 & 1 & 1 \\ 2 & 5 & 3 \end{bmatrix} b2 - {}^{1}/_{4}\, b1 = \begin{bmatrix} 4 & 1 & 3 \\ 0 & {}^{3}/_{4} & {}^{1}/_{4} \\ 2 & 5 & 3 \end{bmatrix} b3 - {}^{1}/_{2}\, b1$$

$$= \begin{bmatrix} 4 & 1 & 3 \\ 0 & {}^{3}/_{4} & {}^{1}/_{4} \\ 0 & {}^{9}/_{2} & {}^{3}/_{2} \end{bmatrix} b3 - 6b2$$

$$= \begin{bmatrix} 4 & 1 & 3 \\ 0 & {}^{3}/_{4} & {}^{1}/_{4} \\ 0 & 0 & 0 \end{bmatrix},$$

Hasil pencarian dengan menggunakan OBE diperoleh rank matriks $A = r(A) = 2$.

Setelah diketahui bahwa rank yang terdapat pada matriks $A = 2$ maka matriks M berukuran 2×2. Sedangkan untuk elemen pada matriks M diambil sebarang pada matriks A yang merupakan bagian kecil dari matriks A.

Selanjutnya diambil matriks $M = \begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix}$

$\det M = \begin{bmatrix} 4 & 1 \\ 1 & 1 \end{bmatrix} = \big((4)(1)\big) - \big((1)(1)\big) = 4 - 1 = 3$

$M^{-1} = {}^{1}/_{3} \begin{bmatrix} 1 & -1 \\ -1 & 4 \end{bmatrix} = \begin{bmatrix} {}^{1}/_{3} & {}^{-1}/_{3} \\ {}^{-1}/_{3} & {}^{4}/_{3} \end{bmatrix}$

$(M^{-1})^{T} = \begin{bmatrix} {}^{1}/_{3} & {}^{-1}/_{3} \\ {}^{-1}/_{3} & {}^{4}/_{3} \end{bmatrix}$

$\begin{bmatrix} {}^{1}/_{3} & {}^{-1}/_{3} & 0 \\ {}^{-1}/_{3} & {}^{4}/_{3} & 0 \\ 0 & 0 & 0 \end{bmatrix}$ transpose $G = \begin{bmatrix} {}^{1}/_{3} & {}^{-1}/_{3} & 0 \\ {}^{-1}/_{3} & {}^{4}/_{3} & 0 \\ 0 & 0 & 0 \end{bmatrix}$

Pembuktian $AGA = A$

$AG = \begin{bmatrix} 4 & 1 & 3 \\ 1 & 1 & 1 \\ 2 & 5 & 3 \end{bmatrix} \begin{bmatrix} {}^{1}/_{3} & {}^{-1}/_{3} & 0 \\ {}^{-1}/_{3} & {}^{4}/_{3} & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 6 & 0 \end{bmatrix}$

$AGA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 6 & 0 \end{bmatrix} \begin{bmatrix} 4 & 1 & 3 \\ 1 & 1 & 1 \\ 2 & 5 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 1 & 3 \\ 1 & 1 & 1 \\ 2 & 5 & 3 \end{bmatrix}$. ■

2.4 Aritmatika Modulo

Aritmatika modulo merupakan operasi matematika yang banyak diimplementasikan pada metode kriptografi karena nilai matematika aritmatika modulo berada dalam himpunan berhingga (0 sampai m – 1). Operator yang digunakan pada aritmatika modulo adalah $\boldsymbol{mod}$.

Defenisi 2.2 (Rinaldi Munir, 2007) Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $a \bmod m$ (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Dengan kata lain, $a \bmod m = r$ sedemikian sehingga $a = mq + r$. dengan $0 \leq r < m$.

Contoh 2.5 :

Carilah sisa modulo dari

(a) $23\ mod\ 5$ (d) $0\ mod\ 12$

(b) $27\ mod\ 3$ (c) $-\ 41\ mod\ 9$

(c) $6\ mod\ 8$

Penyelesaian :

$23\ mod\ 5\ =\ 3\ \ karena\ (23\ =\ 5\ x\ 4\ +\ 3)$.

$27\ mod\ 3\ =\ 0\ karena\ (27\ =\ 3\ x\ 9\ +\ 0)$.

$6\ mod\ 8\ =\ 6\ karena\ (6\ =\ 8\ x\ 0\ +\ 6)$.

$0\ mod\ 12 = 12\ karena\ \ (0\ =\ 12\ x\ 0\ +\ 12)$.

$-\ 41\ mod\ 9\ = 4\ karena\ \ (-41\ =\ 9\ (-5)\ +\ 4)$.

2.4.1 Kongruen

Terkadang dua buah bilangan bulat a dan b, mempunyai sisa yang sama jika dibagi dengan bilangan bulat positif m. Dikatakan bahwa a dan b kongruen dalam modulo m, dan dilambangkan sebagai $a \equiv b(mod\ m)$. Notasi '≡' dibaca kongruen.

Defenisi 2.3 (Rinaldi Munir, 2007) Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b(mod\ m)$ jika m habis membagi $a - b$.

Contoh 2.6:

Carilah kekongruenan modulo dari

(a) $17\ mod\ 3$

(b) $12\ mod\ 7$

Penyelesaian :

$17 \equiv 2(mod\ 3)$ (3 habis membagi $17 - 2 = 15 \rightarrow 15 \div 3 = 5$).

$12 \equiv /2(mod\ 7)$ (7 tidak habis membagi $12 - 2 = 10$).

Kongruen $a \equiv b\ (mod\ m)$ dapat pula ditulis dalam hubungan $a = b + km$. Yang dalam hal ini sembarang k adalah bilangan bulat. Beberapa hasil operasi dengan operator modulo berikut :

$0\ mod\ 12 = 12$ dapat ditulis sebagai $0 \equiv 0\ (mod\ 12)$.

$-39\ mod\ 13 = 0$ dapat ditulis sebagai $-39 \equiv 0 (mod\ 13)$.

Teorema 2.6 (Rinaldi Munir. 2007) Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b\ (mod\ m)$ dan c adalah sembarang bilangan bulat maka:
   i. $(a + c) \equiv (b + c)(mod\ m)$.
   ii. $ac \equiv bc\ (mod\ m)$.
   iii. $a^P \equiv b^P (mod\ m)$ *untuk suatu bilangan bulat tak negatif* P.
2. Jika $a \equiv b\ (mod\ m)$ dan $c \equiv d\ (mod\ m)$, maka
   i. $(a + c) \equiv (b + d)(mod\ m)$.
   ii. $ac \equiv bd\ (mod\ m)$.

Bukti :

1. i. Diketahui $a \equiv b\ (mod\ m)$ dan c adalah sembarang bilangan bulat. Akan ditunjukkan $(a + c) \equiv (b + c)(mod\ m)$.

   $a \equiv b\ (mod\ m)$ berarti :

   $\leftrightarrow a = b + km$

   $\leftrightarrow a - b = km$

   $\leftrightarrow (a - b) + c = (+c)km$

   $\leftrightarrow (a + c) = (b + c) + km$

   $\leftrightarrow (a + c) = (b + c)\ (mod\ m)$.

   ■

   ii. Diketahui $a \equiv b\ (mod\ m)$ dan c adalah sembarang bilangan bulat. Akan ditunjukkan $ac \equiv bc(mod\ m)$.

   $a \equiv b\ (mod\ m)$ berarti :

   $\leftrightarrow a = b + km$

   $\leftrightarrow a - b = km$

   $\leftrightarrow (a - b)c = ckm$

$\leftrightarrow ac = bc + ckm$

$\leftrightarrow ac = bc + Km$

$\leftrightarrow ac = bc \ (mod\ m)$. ■

iii. Diketahui $a \equiv b\ (mod\ m)$ dan c adalah sembarang bilangan bulat. Akan ditunjukkan $a^P \equiv b^P (mod\ m)$.

Untuk bukti ini kita gunakan induksi matematika.

Untuk $p = 1$, berlaku $a \equiv b\ (mod\ m)$.

Asumsikan $a^p = b^p (mod\ m)$ berlaku,

harus ditunjukkan $a^{p+1} = b^{p+1} (mod\ m)$ juga berlaku.

Dari pembuktian 2(ii) Jika $a \equiv b\ (mod\ m)$ dan $c \equiv d\ (mod\ m)$, maka $ac \equiv bd\ (mod\ m)$. Kita ganti c dengan a^pdan d dengan b^pdiperoleh $aa^p = bb^p (mod\ m)$ hal ini akan membuktikan $a^{p+1} = b^{p+1} (mod\ m)$ juga berlaku. ■

2. i. Diketahui $a \equiv b\ (mod\ m)$ dan $c \equiv d\ (mod\ m)$. Akan ditunjukkan $(a + c) \equiv (b + d) (mod\ m)$.

$a \equiv b\ (mod\ m) \leftrightarrow a = b + k_1 m$

$c \equiv d\ (mod\ m) \leftrightarrow \underline{c = d + k_2 m} +$

$\leftrightarrow (a + c) = (b + d) + (k_1 + k_2)m$

$\leftrightarrow (a + c) = (b + d) + km$

$\leftrightarrow (a + c) = (b + d) (mod\ m)$. ■

ii. Diketahui $a \equiv b\ (mod\ m)$ dan $c \equiv d\ (mod\ m)$. Akan ditunjukkan $ac \equiv bd\ (mod\ m)$.

$a \equiv b\ (mod\ m) \leftrightarrow a = b + k_1 m$

$c \equiv d\ (mod\ m) \leftrightarrow c = d + k_2 m$

$ac = (b + k_1 m)(d + k_1 m)$

$ac = bd + bk_2 m + dk_1 m + k_1 m k_2 m$

$ac = bd + (bk_2 + dk_1 + k_1 k_2 m)m$

karena $(bk_2 + dk_1 + k_1k_2m)$ bilangan bulat maka nilainya dapat diganti dengan K, sehingga

$ac = bd + Km$

$ac = bd + (mod\ m)$. ■

Contoh 2.7:

Hitunglah aritmatika modulo berpangkat 572^{37}.

Penyelesaian :

$572^{37} = 572^{36} \times 572 = 572^{32} \times 572^4 \times 572.$

$572^2\ mod\ 713 = 327184\ mod\ 713 = 630.$

$572^4\ mod\ 713 = 572^2 \times 572^2\ mod\ 713$

$= [(572^2\ mod\ 713)(572^2\ mod\ 713)]\ mod\ 713$

$= 630^2\ mod\ 713 = 396900\ mod\ 713 = 472.$

$572^8\ mod\ 713 = 572^4 \times 572^4\ mod\ 713$

$= [(572^4\ mod\ 713)(572^4\ mod\ 713)]\ mod\ 713$

$= 472^2\ mod\ 713 = 222784\ mod\ 713 = 328.$

$572^{16}\ mod\ 713 = 572^8 \times 572^8\ mod\ 713$

$= [(572^8\ mod\ 713)(572^8\ mod\ 713)]\ mod\ 713$

$= 328^2\ mod\ 713 = 107584\ mod\ 713 = 634.$

$572^{32}\ mod\ 713 = 572^{16} \times 572^{16} mod\ 713$

$= [(572^{16}\ mod\ 713)(572^{16}\ mod\ 713)]\ mod\ 713$

$= 634^2\ mod\ 713 = 401956\ mod\ 713 = 537.$

2.4.2 Invers Modulo

Setiap bilangan tak-nol a mempunyai balikan atau invers perkalian. Yang dinyatakan dengan a^{-1}, sedemikian rupa sehingga $aa^{-1} = a^{-1}a = 1$. begitu pula konsep pada aritmatika modular.

Defenisi 2.4 (Anton, Howard. 1998) Jika a adalah suatu bilangan dalam Z_m, maka bilangan a^{-1} dalam Z_m disebut balikan atau invers perkalian dari a modulo m jika $aa^{-1} = a^{-1}a = 1(mod\ m)$.

Teorema 2.7 (Anton, Howard. 1998) Matriks bujur sangkar A dengan elemen-elemen di Z_m adalah modulo m yang dapat dibalikkan jika dan hanya jika sisa dari $\det(A)$ modulo m mempunyai balikan modulo m.

Bukti :

Misalkan matriks $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ mempunyai elemen di Z_{29} dan sisa dari $\det(A) = ad - bc$ modulo 29 tidak habis dibagi oleh bilangan prima, maka balikan dari $A(mod\ 29)$ diberikan oleh

$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (mod\ 29)$ dimana $(ad - bc)^{-1}$ adalah balikan dari sisa $ad - bc\ (mod\ 29)$. ■

Contoh 2.8 :

Diberikan matriks $A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$

Carilah invers modular dari matriks A bila diketahui operator modulo yang digunakan 26.

Penyelesaian :

$$\det(A) = ad - bc = (5)(3) - (6)(2) = 3$$

sehingga,

$$(ad - bc)^{-1} = 3^{-1} = 9(mod\ 26)$$

Jadi,

$$A^{-1} = 9 \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -18 & 45 \end{bmatrix} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} (mod\ 26).$$

2.5 Kriptografi

Sebelum membahas tentang algoritma yang akan digunakan, terlebih dahulu dibahas tentang kriptografi.

Defenisi 2.5 (Manezes dkk, 1997) Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti keabsahan, integritas data, serta autentifikasi data.

Kriptografi mempunyai beberapa algoritma yang pada dasarnya terdiri dari dua bagian. Bagian ini yang akan membedakan model pada kriptografi. Model yang pertama dikenal dengan model kriptografi yang menggunakan kunci sama saat proses enkripsi dan pada saat proses dekripsi dan model yang kedua yaitu model kriptografi yang menggunakan dua buah kunci (*key*) yang berbeda saat enkripsi (*encryption*) dan dekripsi (*decryption*) data. Berdasarkan sifat kuncinya tersebut maka terdapat dua jenis algoritma kriptografi yaitu algoritma simetris dan algoritma asimetris.

2.5.1 Algoritma Simetris

Algoritma simetris disebut juga sebagai algoritma konvensional. Suatu algoritma dikatakan algoritma simetris apabila pasangan kunci untuk proses enkripsi dan dekripsinya adalah sama. Contoh dari algoritma simetris adalah Vigenere Cipher, Cipher Permutasi, Cipher Substitusi, Hill Cipher dan lain-lain.

2.5.2 Algoritma Asimetris

Algoritma asimetris adalah algoritma yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun diantara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu bahkan jika mereka saling tidak mengenal satu sama lainnya. Contoh dari algoritma asimetris adalah DH (Diffie-Hellman), RSA, El-gamal dan lain-lain.

Tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut :

a. *Confidelity* (kerahasiaan).

b. *Data Integrity* (keutuhan data).

c. *Authentication* (keotentikan).

d. *Non-Repudiation* (anti penyangkalan).

Kehidupan kita sehari-hari dikelilingi oleh kriptografi, beberapa diantaranya yakni :

a. *Smatr Card.*

b. ATM.

c. *Cell-Phone.*

2.6 Diffie-Hellman (DH)

Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada tahun 1976 saat Diffie dan Hellman mempublikasikan *"New Directions in Cryptography"*. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan.

Diffie-Hellman (DH) dianggap merupakan algoritma kunci publik yang pertama kali. Algoritma Diffie-hellman (DH) hanya dapat digunakan untuk pertukaran kunci (simetris) dan tidak dapat digunakan untuk enkripsi/ dekripsi maupun untuk tanda tangan digital. Diffie-Hellman membuat algoritma pertukaran kunci yang keamanannya didasarkan pada fakta bahwa menghitung logaritma diskrit sangat sulit.

Tujuan utama dari algoritma ini adalah membuat dua pengguna bertukar kunci secara aman sehingga kemudian dapat digunakan untuk enkripsi pesan. Algoritma ini sendiri terbatas pada penukaran kunci.

Salah satu contoh masalah dalam penyandian yang diselesaikan menggunakan algoritma ini adalah " dimisalkan Pengguna Pertama dan Pengguna Kedua ingin berbagi kunci rahasia untuk digunakan dalam cipher simetris, tetapi alat komunikasi mereka tidak aman. Setiap bagian dari informasi yang mereka tukar diamati oleh musuh mereka. Bagaimana mungkin Pengguna Pertama dan Pengguna Kedua untuk berbagi kunci tanpa sepengetahuan Musuh? Sepintas

tampak bahwa Pengguna Pertama dan Pengguna Kedua menghadapi tugas yang mustahil". Permasalahan seperti ini lah yang membuat Diffie-Hellman membentuk algoritma pertukaran kunci.

Penyelesaian permasalahan tersebut dapat diselesaikan dengan protokol pertukaran kunci Diffie-Hellman sebagai berikut :

1. Mula-mula Pengguna Pertama dan Pengguna Kedua menyepakati bilangan prima yang besar, n dan g, sedemikian sehingga $g < n$. Bilangan n dan g tidak perlu rahasia. Bahkan, Pengguna Pertama dan Pengguna Kedua dapat membicarakannya melalui saluran yang tidak aman sekalipun.
2. Pengguna Pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada Pengguna Kedua: $X = g^x \bmod n$.
3. Pengguna Kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada Pengguna Pertama: $Y = g^y \bmod n$.
4. Pengguna Pertama menghitung $K = Y^x \bmod n$.
5. Pengguna Kedua menghitung $K' = X^y \bmod n$.

Jika perhitungan dilakukan dengan benar, maka $K = K'$. Baik K dan K' sama dengan $g^{xy} \bmod n$. Musuh yang mendengarkan semua hal selama protokol berlangsung tidak dapat menghitung kunci K. Ia hanya memiliki informasi n, g, X dan Y, tetapi ia tidak mempunyai informasi nilai x dan y. Ia perlu melakukan perhitungan logaritma diskrit, yang mana sangat sulit dikerjakan untuk mengetahui x atau y.

BAB III
METODOLOGI PENELITIAN

Adapun metode penelitian yang penulis gunakan adalah metode studi literatur dengan langkah-langkah sebagai berikut:

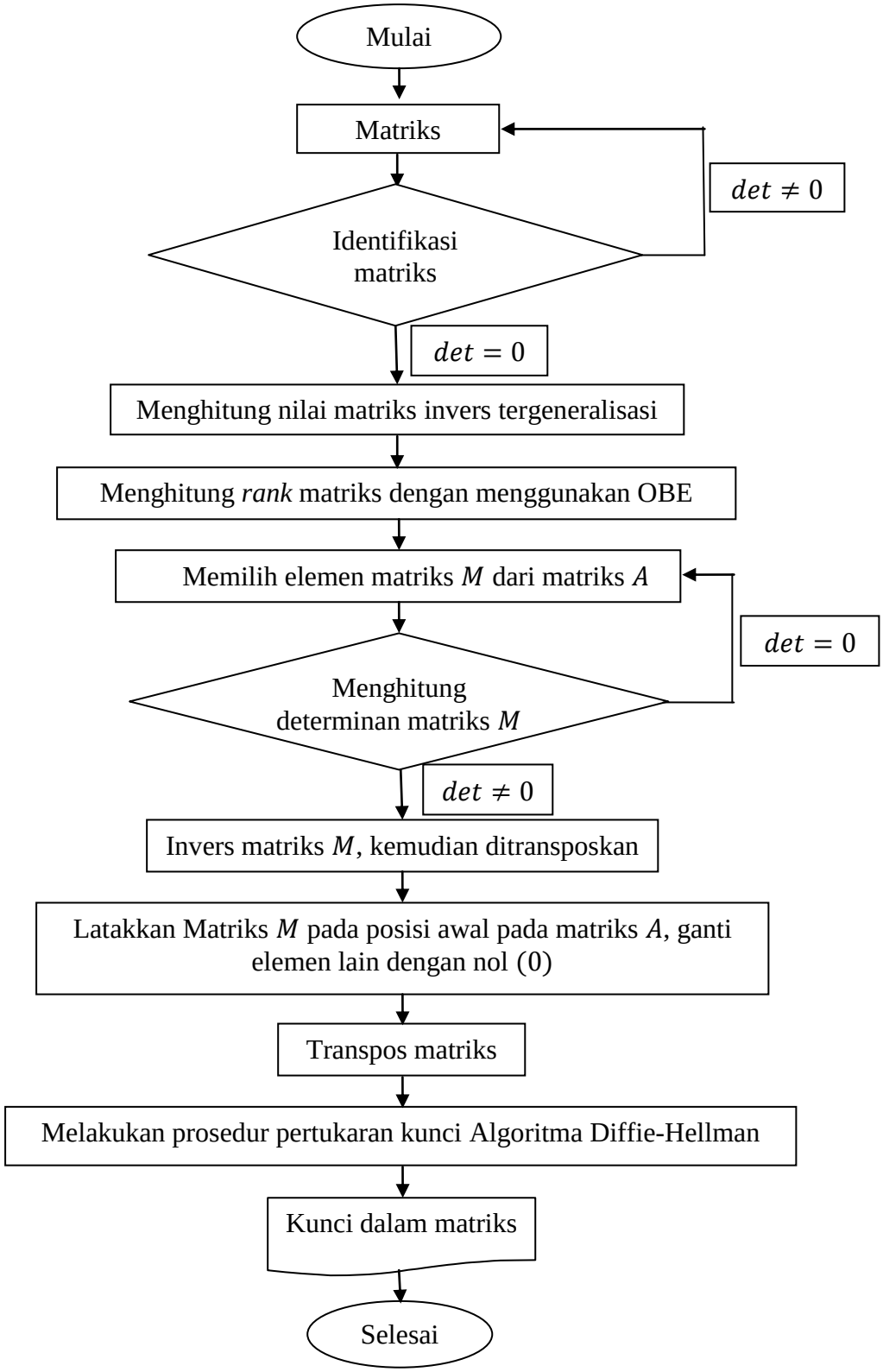
1. Memilih atau membentuk sebarang matriks kuadrat dan operaton modulo.
2. Identifikasi Matriks. Jika determinan bernilai nol ($det = 0$) maka akan dilanjutkan pada langkah selanjutnya. Namun, jika determinan bernilai tidak sama dengan nol ($det \neq 0$) maka kembali pada langkah sebelumnya.
3. Menghitung nilai matriks invers tergeneralisasi.
    a. Menghitung *rank* matriks dengan menggunakan OBE.
    b. Memilih elemen matriks M dari matriks A (sebarang matriks yang telah diidentifikasi) dengan ordo yang berasal dari nilai *rank* yang diperoleh dari proses OBE.
    c. Menghitung determinan matriks M yang merupakan cerminan matriks non-singular. Jika terbukti bahwa matriks tersebut non-singular maka langkah dapat dilanjutkan. Namun jika matriks tersebut singular maka pemilihan matriks M akan diubah (kembali pada sublangkah b).
    d. Invers matriks M, kemudian ditransposkan.
    e. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks M diambil dari matriks A.
    f. Mengganti semua elemen lain dengan nol.
    g. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi, matriks ini disebut matriks g.
4. Melakukan prosedur pertukaran kunci.
    a. Pengguna Pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada Pengguna Kedua:
    $X = g^x \ mod \ n.$

b. Pengguna Kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada Pengguna Pertama: $Y = g^y \ mod \ n.$

c. Pengguna Pertama menghitung
$K = Y^x \ mod \ n.$

d. Pengguna Kedua menghitung
$K' = X^y \ mod \ n.$

Langkah-langkah tersebut di atas digambarkan dalam *flowchart* di bawah ini:



Gambar 3.1 *Flowchart* Metode Penelitian.

BAB IV
PEMBAHASAN DAN HASIL

Bab IV ini akan membahas tentang pembentukan kunci dengan aplikasi matriks invers tergeneralisasi pada Diffie-Hellman. Pertukaran kunci berlangsung antara oleh Pengguna Pertama dan Pengguna Kedua yang melakukan beberapa kesepakatan.

4.1 Aplikasi Matriks Invers Tergeneralisasi pada Diffie-Hellman.

Berikut ini akan dijelaskan tentang bagaimana pengaplikasian matriks invers tergeneralisasi pada Diffie-Hellman. Algoritma Diffie-Hellman pada dasarnya menggunakan teori bilangan yang sangat besar pada pertukaran kuncinya. Namun pada umumnya proses pembentukan sebuah pesan menjadi tidak dapat dibaca menggunakan kunci (*key*) berupa matriks, maka untuk pengembangan penggunaan algoritma Diffie-Hellman bilangan yang sangat besar tersebut diganti dengan matriks. Sementara itu, matriks invers tergeneralisasi memiliki hal yang unik untuk diaplikasikan pada proses pertukaran kunci dengan menggunakan algoritma Diffie-Hellman.

Sesuai penjelasan pada bab II, bahwa Diffie-Hellman adalah sebuah algoritma pertukaran kunci yang dilakukan oleh dua pengguna yang melakukan kesepakatan tertentu yang dalam skripsi ini kesepakatan tersebut berupa :

1. Ordo matriks.
2. Nilai pada elemen matriks.
3. Matriks invers tergeneralisasi berupa letak *rank* yang digunakan.
4. Operator modulo yang digunakan.

Penyelesaian pembentukan kunci terdiri dari langkah-langkah sebagai berikut :

4.1.1 Identifikasi Matriks

Langkah ini dilakukan untuk mengidentifikasi sebuah matriks singular atau non-singular. Matriks dikatakan singular jika $det = 0$, sebaliknya matriks

dikatakan non-singuler jika $det \neq 0$. Identifikasi ini dilakukan untuk memenuhi syarat dari matriks invers tergeneralisasi yaitu matriks singular.

4.1.2 Matriks Invers Tergeneralisasi

Matriks invers tergeneralisasi ini merupakan perluasan dari invers matriks. Ketentuan umum untuk invers matriks yaitu matriks non-singular. Namun faktanya tidak semua matriks tersebut non-singular. Alasan tersebut yang menjadi dasar terciptanya matriks invers tergeneralisasi dengan sublangkah yaitu dalam jurnal *On The Generalisized Inverse of a Matrikx* (Adetunde dkk, 2010) :

1. Menghitung *rank* matriks dengan menggunakan OBE.
2. Memilih elemen matriks M dari matriks A (sebarang matriks yang telah diidentifikasi) dengan ordo yang berasal dari nilai *rank* yang diperoleh dari proses OBE.
3. Menghitung determinan matriks M yang merupakan cerminan matriks non-singular. Jika terbukti bahwa matriks tersebut non-singular maka langkah dapat dilanjutkan. Namun jika matriks tersebut singular maka pemilihan matriks M akan diubah (kembali pada sublangkah b).
4. Invers matriks M, kemudian ditransposkan.
5. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks M diambil dari matriks A.
6. Mengganti semua elemen lain dengan nol.
7. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi, matriks ini disebut matriks g.

Berdasarkan penguraian di atas, dapat diperoleh ketentuan-ketentuan sebagai berikut :

1. Jika matriks M nilai $\det(M) = 1$ atau $\det(M) = -1$, maka proses dilanjutkan pada langkah pertukaran kunci.
2. Jika matriks M nilai $\det(M) < -1$ atau $\det(M) > 1$, maka dilakukan pencarian dengan menggunakan invers aritmatika modulo kemudian dilanjutkan pada langkah pertukaran kunci.

3. Jika kesepakatan letak *rank* matriks yang disebut matriks M juga mempunyai nilai determinan sama dengan nol, maka kesepakatan untuk letak *rank* akan diubah.

Perhitungan pada matriks invers tergeneralisasi ini juga dipengaruhi oleh aritmatika modulo, karena pada pertukaran kunci terdapat syarat bahwa elemen pada matriks tidak lebih besar dari pada nilai operator modulo yang disepakati.

4.1.3 Prosedur Pertukaran Kunci Diffie-Hellman

Berdasarkan penjelasan sebelumnya, pada prosedur pertukaran kunci memerlukan beberapa kesepakatan. Kesepakatan dalam skripsi ini akan diaplikasikan pada protokol pertukaran kunci. Berikut protokol tersebut :

a. Pengguna pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada pengguna kedua:
   $X = g^x \ mod \ n.$
b. Pengguna kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada pengguna pertama:
   $Y = g^y \ mod \ n.$
c. Pengguna pertama menghitung
   $K = Y^x \ mod \ n.$
d. Pengguna kedua menghitung
   $K' = X^y \ mod \ n.$

4.2 Contoh Aplikasi Matriks Invers Tergeneralisasi pada Diffie-Hellman.

Misalkan pengguna pertama dan pengguna kedua ingin berbagi kunci rahasia untuk digunakan dalam cipher simetris, tetapi alat komunikasi mereka tidak aman. Setiap bagian dari informasi yang mereka tukar diamati oleh musuh mereka. Bagaimana mungkin pengguna pertama dan pengguna kedua untuk berbagi kunci tanpa sepengetahuan musuh?

Contoh 4.1 (Untuk $det\ (M) = 1$ atau $det\ (M) = -1$)

Diberikan kesepakatan sebagai berikut :

1. Ordo matriks yaitu ordo 4.
2. Elemen matriks $A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$.
3. Letak *rank* matriks yaitu kiri atas.
4. Operator modulo yang digunakan yaitu $mod = 29$.

Penyelesaian :

Langkah 1 : Identifikasi Matriks

Metode yang digunakan untuk identifikasi matriks adalah metode kofaktor.

Diketahui matriks $A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$.

Metode kofaktor merupakan perkalian antara (-1) yang berpangkatkan jumlah koefisien baris dan kolom dari elemen matriks dengan elemen matriks itu sendiri dan determinan dari matriks yang dapat diperoleh dengan perhitungan sarrus.

$$det\ A = (-1)^{1+1}(2)\begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix} + (-1)^{1+2}(4)\begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$$

$$+(-1)^{1+3}(3)\begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix} + (-1)^{1+4}(2)\begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$$

$$= 2\begin{vmatrix} 6 & 5 & 2 \\ 5 & 2 & -3 \\ 5 & 14 & 9 \end{vmatrix} - 4\begin{vmatrix} 3 & 5 & 2 \\ 2 & 2 & -3 \\ 4 & 14 & 9 \end{vmatrix} + 3\begin{vmatrix} 3 & 6 & 2 \\ 2 & 5 & -3 \\ 4 & 5 & 9 \end{vmatrix} - 2\begin{vmatrix} 3 & 6 & 5 \\ 2 & 5 & 2 \\ 4 & 5 & 14 \end{vmatrix}$$

Karena ordo pada matriks ini besar maka metode kofaktor digunakan berulang-ulang hingga diperoleh matriks yang dapat dicari determinannya dengan metode sarrus.

$$= \left((12)\begin{vmatrix} 2 & -3 \\ 14 & 9 \end{vmatrix} + (-10)\begin{vmatrix} 5 & -3 \\ 5 & 9 \end{vmatrix} + (4)\begin{vmatrix} 5 & 2 \\ 5 & 14 \end{vmatrix}\right) -$$

$$\left((12)\begin{vmatrix}2 & -3\\14 & 9\end{vmatrix}+(-20)\begin{vmatrix}2 & -3\\4 & 9\end{vmatrix}+(8)\begin{vmatrix}2 & 2\\4 & 14\end{vmatrix}\right)+$$

$$\left((9)\begin{vmatrix}5 & -3\\5 & 9\end{vmatrix}+(-18)\begin{vmatrix}2 & -3\\4 & 9\end{vmatrix}+(6)\begin{vmatrix}2 & 5\\4 & 5\end{vmatrix}\right)-$$

$$\left((6)\begin{vmatrix}5 & 2\\5 & 14\end{vmatrix}+(-12)\begin{vmatrix}2 & 2\\4 & 14\end{vmatrix}+(10)\begin{vmatrix}2 & 5\\4 & 5\end{vmatrix}\right)$$

$$= (720 - 600 + 240) - (720 - 600 + 160) + (540 - 540 + (-60)$$
$$+(360 - 240 + (-100)$$
$$= 0.$$

Jadi, hasil determinan dari matriks yang disepakati tersebut sama dengan 0 (nol) yang berarti syarat untuk matriks invers tergeneralisasi terpenuhi. Maka proses dapat dilanjutkan pada langkah selanjutnya.

Langkah 2 : Matriks Invers Tergeneralisasi.

Langkah ini dalam protokol pertukaran kunci diperoleh pada masing-masing pengguna yang melakukan pertukaran kunci, karena pada kesepakatan hanya menggunakan matriks biasa. Langkah ini akan diselesaikan dengan beberapa sublangkah dari pembentukan matriks invers tergeneralisasi. Uraian sublangkah tersebut yaitu :

1. Menghitung *rank* matriks dengan menggunakan OBE.

   Diketahui matriks

   $A = \begin{bmatrix}2 & 4 & 3 & 2\\3 & 6 & 5 & 2\\2 & 5 & 2 & -3\\4 & 5 & 14 & 9\end{bmatrix}$, berikut perhitungan dengan menggunakan OBE

   a. Mengurangkan baris ke-2 dengan $\frac{3}{2}$ kali baris ke-1

   $$A = \begin{bmatrix}2 & 4 & 3 & 2\\3 & 6 & 5 & 2\\2 & 5 & 2 & -3\\4 & 5 & 14 & 9\end{bmatrix} b2 - \tfrac{3}{2}b1$$

   $$= \begin{bmatrix}2 & 4 & 3 & 2\\3 & 6 & 5 & 2\\2 & 5 & 2 & -3\\4 & 5 & 14 & 9\end{bmatrix}$$

b. Mengurangkan baris ke-3 dengan baris ke-1

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 0 & 1/2 & -1 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix} b3 - b1$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 0 & 1/2 & -1 \\ 0 & 1 & -1 & -5 \\ 4 & 5 & 14 & 9 \end{bmatrix}$$

c. Mengurangkan baris ke-4 dengan 2 kali baris ke-1

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 0 & 1/2 & -1 \\ 0 & 1 & -1 & -5 \\ 4 & 5 & 14 & 9 \end{bmatrix} b4 - 2b1$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 0 & 1/2 & -1 \\ 0 & 1 & -1 & -5 \\ 0 & -3 & 8 & 5 \end{bmatrix}$$

d. Menukarkan baris ke-2 dengan baris ke-3

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 0 & 1/2 & -1 \\ 0 & 1 & -1 & -5 \\ 0 & -3 & 8 & 5 \end{bmatrix} \text{ tukar } b2 \text{ dengan } b3$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 1 & -1 & -5 \\ 0 & 0 & 1/2 & -1 \\ 0 & -3 & 8 & 5 \end{bmatrix}$$

e. Mengurangkan baris ke-4 dengan 3 kali baris ke-2

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 1 & -1 & -5 \\ 0 & 0 & 1/2 & -1 \\ 0 & -3 & 8 & 5 \end{bmatrix} b4 - 3b2$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 1 & -1 & -5 \\ 0 & 0 & 1/2 & -1 \\ 0 & 0 & 5 & -10 \end{bmatrix}$$

f. Mengurangkan baris ke-4 dengan 10 kali baris ke-3

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 1 & -1 & -5 \\ 0 & 0 & {}^{1}/_{2} & -1 \\ 0 & 0 & 5 & -10 \end{bmatrix} b4 - 10b3$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 0 & 1 & -1 & -5 \\ 0 & 0 & {}^{1}/_{2} & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Hasil perhitungan di atas dengan menggunakan OBE diperoleh *rank* matriks $A = r(A) = 3$. Maka ordo untuk matriks M adalah matriks 3×3.

2. Menghitung determinan matriks M yang merupakan cerminan matriks non-singular.

Matriks M merupakan matriks minor dari matriks A yang letak pengambilannya merupakan suatu kesepakatan. Berikut matriks dari kesepakatan tersebut:

$$M = \begin{bmatrix} 2 & 4 & 3 \\ 3 & 6 & 5 \\ 2 & 5 & 2 \end{bmatrix}$$

Pembuktian bahwa matriks ini merupakan cerminan matriks non-singular yaitu menggunakan kofaktor.

$$\det M = (-1)^{1+1}(2)\begin{bmatrix} 2 & 4 & 3 \\ 3 & 6 & 5 \\ 2 & 5 & 2 \end{bmatrix} + (-1)^{1+2}(4)\begin{bmatrix} 2 & 4 & 3 \\ 3 & 6 & 5 \\ 2 & 5 & 2 \end{bmatrix}$$

$$+(-1)^{1+3}(3)\begin{bmatrix} 2 & 4 & 3 \\ 3 & 6 & 5 \\ 2 & 5 & 2 \end{bmatrix}$$

$$= 2\begin{vmatrix} 6 & 5 \\ 5 & 2 \end{vmatrix} + (-4)\begin{vmatrix} 3 & 5 \\ 2 & 2 \end{vmatrix} + 3\begin{vmatrix} 3 & 6 \\ 2 & 5 \end{vmatrix}$$

$$= 2(12 - 25) + (-4)(6 - 10) + 3(15 - 12)$$

$$= -1$$

Terbukti bahwa determinan matriks di atas $\neq 0$, maka proses dapat dilanjutkan pada langkah selanjutnya.

3. Invers matriks M, kemudian tansposkan.

   Invers matrik M dapat dicari dengan menggunakan metode adjoin sebagai berikut :

$$M = \begin{bmatrix} 2 & 4 & 3 \\ 3 & 6 & 5 \\ 2 & 5 & 2 \end{bmatrix}$$

$$M^{-1} = \frac{1}{\det M}[adj\ M]$$

$$[adj\ M] = \begin{bmatrix} k_{11} & k_{21} & k_{31} \\ k_{12} & k_{22} & k_{32} \\ k_{13} & k_{23} & k_{33} \end{bmatrix} = \begin{bmatrix} -13 & 7 & 2 \\ 4 & -2 & -1 \\ 3 & -2 & 0 \end{bmatrix}$$

$$M^{-1} = \frac{1}{-1} = \begin{bmatrix} -13 & 7 & 2 \\ 4 & -2 & -1 \\ 3 & -2 & 0 \end{bmatrix} = \begin{bmatrix} 13 & -7 & -2 \\ -4 & 2 & 1 \\ -3 & 2 & 0 \end{bmatrix}$$

$$(M^{-1})^T = \begin{bmatrix} 13 & -4 & -3 \\ -7 & 2 & 2 \\ -2 & 1 & 0 \end{bmatrix}.$$

4. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks *M* diambil dari matriks A. Mengganti semua elemen lain dengan nol. Matriks disebut G

$$G = \begin{bmatrix} 13 & -4 & -3 & 0 \\ -7 & 2 & 2 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

5. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi.

$$G = \begin{bmatrix} 13 & -4 & -3 & 0 \\ -7 & 2 & 2 & 0 \\ -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$G^T = g = \begin{bmatrix} 13 & -7 & -2 & 0 \\ -4 & 2 & 1 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

   bukti bahwa matriks di atas adalah matriks invers tergeneralisasi yaitu memenuhi sifat :

   a) $gAg = g$.

b) $AgA = A$.

Bukti :

$$g = \begin{bmatrix} 13 & -7 & -2 & 0 \\ -4 & 2 & 1 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$$

$$Ag = \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix} \begin{bmatrix} 13 & -7 & -2 & 0 \\ -4 & 2 & 1 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -10 & 10 & -3 & 0 \end{bmatrix}$$

$$AgA = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -10 & 10 & -3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 9 \end{bmatrix}.$$

■

Langkah 3 : Pertukaran Kunci Diffie-Hellman

Mengaplikasikan semua kesepakatan yang telah dibuat dengan melakukan proses pada protokol pertukaran kunci Diffie-Hellman sebagai berikut :

1. Pengguna pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada pengguna kedua sebagai berikut :

   $X = g^x \bmod n.$

   Bilangan bulat yang dipilih oleh pengguna pertama hanya pengguna pertama yang tahu. Misalkan pengguna pertama memilih bilangan bulat $x = 15$, maka perhitungan X yang diperoleh yaitu :

$$X = \begin{bmatrix} 13 & -7 & -2 & 0 \\ -4 & 2 & 1 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}^{15} \ mod\ 29$$

Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13.*

Maka diperoleh matriks X yaitu :

$$X = \begin{bmatrix} 24 & 11 & 23 & 0 \\ 5 & 28 & 0 & 0 \\ 10 & 9 & 23 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran A.

2. Pengguna kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada pengguna pertama:

   $Y = g^y \ mod\ n.$

   Sama halnya dengan pengguna pertama, bilangan bulat yang dipilih oleh pengguna kedua hanya pengguna kedua yang tahu. Misalkan pengguna kedua memilih bilangan bulat $y = 27$, maka perhitungan Y yang diperoleh yaitu :

$$Y = \begin{bmatrix} 13 & -7 & -2 & 0 \\ -4 & 2 & 1 & 0 \\ -3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}^{27} \ mod\ 29$$

   Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13.*

   Maka diperoleh matriks Y yaitu :

$$Y = \begin{bmatrix} 10 & 19 & 10 & 0 \\ 26 & 3 & 11 & 0 \\ 20 & 3 & 27 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

   Proses selengkapnya dapat dilihat pada lampiran B.

3. Pengguna pertama menghitung

   $K = Y^x \ mod\ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K = \begin{bmatrix} 10 & 19 & 10 & 0 \\ 26 & 3 & 11 & 0 \\ 20 & 3 & 27 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}^{15} \ mod\ 29$$

$$= \begin{bmatrix} 18 & 6 & 6 & 0 \\ 14 & 11 & 12 & 0 \\ 1 & 8 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran C.

4. Pengguna kedua menghitung

$K' = X^y \ mod\ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K' = \begin{bmatrix} 24 & 11 & 23 & 0 \\ 5 & 28 & 0 & 0 \\ 10 & 9 & 23 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}^{27} \ mod\ 29$$

$$= \begin{bmatrix} 18 & 6 & 6 & 0 \\ 14 & 11 & 12 & 0 \\ 1 & 8 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran D.

Terlihat bahwa perhitungan dilakukan dengan benar. Hal ini ditunjukkan dengan $K = K' = \begin{bmatrix} 18 & 6 & 6 & 0 \\ 14 & 11 & 12 & 0 \\ 1 & 8 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Jadi, dari semua perhitungan diperoleh K dan K' yang merupakan kunci bersama yang dimiliki oleh pengguna pertama dan pengguna kedua. Kunci ini merupakan kunci rahasia bagi kedua pengguna. Sehingga, kedua pengguna tersebut dapat melakukan pengiriman pesan dalam bentuk *chipper* yang hanya dapat dibaca oleh kedua pengguna yang saling mempunyai kunci yang sama.

Contoh 4.2 (Untuk nilai determinan pada matriks $M < -1$ atau $M > 1$)

Diberikan kesepakatan sebagai berikut :

1. Ordo matriks yaitu ordo 5.
2. Elemen matriks $A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$.
3. Letak *rank* matriks yaitu kiri atas.
4. Operator modulo yang digunakan yaitu $mod = 29$.

Penyelesaian :

Langkah 1 : Identifikasi Matriks

Identifikasi matriks ini menggunakan program *maple 13*.

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$$

$\det A = 0$.

Identifikasi matriks dari kesepakatan tersebut menghasilkan determinan sama dengan nol (0) yang berarti syarat untuk matriks invers tergeneralisasi terpenuhi. Maka proses dapat dilanjutkan pada langkah selanjutnya.

Langkah 2 : Matriks Invers Tergeneralisasi.

1. Menghitung *rank* matriks dengan menggunakan OBE.

   Diketahui matriks $A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$

   berikut perhitungan dengan menggunakan OBE

   a. Mengurangkan baris ke-2 dengan 3 kali baris ke-1

   $$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix} b2 - 3b1$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$$

b. Mengurangkan baris ke-3 dengan 3 kali baris ke-1

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix} b3 - 3b1$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & -4 & 3 & -9 & -2 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$$

c. Mengurangkan baris ke-5 dengan 3 kali baris ke-1

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & -4 & 3 & -9 & -2 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix} b5 - 3b1$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & -4 & 3 & -9 & -2 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix}$$

d. Mengurangkan baris ke-3 dengan $\frac{4}{6}$ kali baris ke-2

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & -4 & 3 & -9 & -2 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix} b3 - \frac{4}{6}b2$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3.7 & 0{,}7 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix}$$

e. Mengurangkan baris ke-4 dengan $\frac{1}{6}$ kali baris ke-1

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3.7 & 0{,}7 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix} b4 - \tfrac{1}{6} b2$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3{,}7 & 0{,}7 \\ 0 & 0 & 2{,}7 & 1{,}7 & 3.3 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix}$$

f. Mengurangkan baris ke-5 dengan baris ke-2

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3{,}7 & 0{,}7 \\ 0 & 0 & 2{,}7 & 1{,}7 & 3.3 \\ 0 & -6 & 4 & -8 & -4 \end{bmatrix} b5 - b2$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3{,}7 & 0{,}7 \\ 0 & 0 & 2{,}7 & 1{,}7 & 3{,}3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

g. Mengurangkan baris ke-4 dengan 8 kali baris ke-3

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3{,}7 & 0{,}7 \\ 0 & 0 & 2{,}7 & 1{,}7 & 3{,}3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} b4 - 8b3$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 0 & -6 & 4 & -8 & -4 \\ 0 & 0 & 0{,}3 & -3{,}7 & 0{,}7 \\ 0 & 0 & 0 & 31 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hasil Perhitungan di atas dengan menggunakan OBE diperoleh *rank* matriks $A = r(A) = 4$. Maka ordo untuk matriks M adalah matriks 4×4.

2. Menghitung determinan matriks M yang merupakan cerminan matriks non-singular.

Matriks M merupakan matriks minor dari matriks A yang letak pengambilannya merupakan suatu kesepakatan. Berikut matriks dari kesepakatan tersebut:

$$M = \begin{bmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix}$$

Pembuktian bahwa matriks ini merupakan cerminan matriks non-singular yaitu menggunakan kofaktor sebagai berikut:

$$\det M = (-1)^{1+1}(1)\begin{vmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{vmatrix} + (-1)^{1+2}(2)\begin{vmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{vmatrix}$$

$$+(-1)^{1+3}(0)\begin{vmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{vmatrix} + (-1)^{1+4}(3)\begin{vmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{vmatrix}$$

$$= \left(1(-1)^{1+1}(0)\begin{vmatrix} 0 & 4 & 1 \\ 2 & 3 & 0 \\ 1 & 2 & 3 \end{vmatrix} + 1(-1)^{1+2}(4)\begin{vmatrix} 0 & 4 & 1 \\ 2 & 3 & 0 \\ 1 & 2 & 3 \end{vmatrix} + \right.$$

$$\left. 1(-1)^{1+3}(1)\begin{vmatrix} 0 & 4 & 1 \\ 2 & 3 & 0 \\ 1 & 2 & 3 \end{vmatrix}\right) - \left(2(-1)^{1+1}(3)\begin{vmatrix} 3 & 4 & 1 \\ 3 & 3 & 0 \\ 0 & 2 & 3 \end{vmatrix} + \right.$$

$$\left. 2(-1)^{1+2}(4)\begin{vmatrix} 3 & 4 & 1 \\ 3 & 3 & 0 \\ 0 & 2 & 3 \end{vmatrix} + 2(-1)^{1+3}(1)\begin{vmatrix} 3 & 4 & 1 \\ 3 & 3 & 0 \\ 0 & 2 & 3 \end{vmatrix}\right) -$$

$$\left(3(-1)^{1+1}(3)\begin{vmatrix} 3 & 0 & 4 \\ 3 & 2 & 3 \\ 0 & 1 & 2 \end{vmatrix} + 3(-1)^{1+2}(0)\begin{vmatrix} 3 & 0 & 4 \\ 3 & 2 & 3 \\ 0 & 1 & 2 \end{vmatrix}\right.$$

$$\left. 3(-1)^{1+3}(4)\begin{vmatrix} 3 & 0 & 4 \\ 3 & 2 & 3 \\ 0 & 1 & 2 \end{vmatrix}\right)$$

$$= (-24 + 1) - (54 - 72 + 12) - (9 + 36)$$

$$= -62$$

Terbukti bahwa determinan matriks di atas $\neq 0$, maka proses dapat dilanjutkan pada langkah selanjutnya.

3. Invers matriks M, kemudian tansposkan.

Invers dan transpos matriks M Menggunakan program *maple 13* yang hasilnya yaitu :

$$M = \begin{bmatrix} 1 & 2 & 0 & 3 \\ 3 & 0 & 4 & 1 \\ 3 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix}$$

$$M^{-1} = \frac{1}{\det M} adj\ M$$

$$= \frac{1}{-62} \begin{bmatrix} -23 & -21 & 8 & 30 \\ 3 & 27 & -28 & -12 \\ 21 & 3 & -10 & -22 \\ -15 & -11 & 16 & -2 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{23}{62} & \frac{21}{62} & -\frac{4}{31} & -\frac{15}{31} \\ -\frac{3}{62} & -\frac{27}{62} & \frac{14}{31} & \frac{6}{31} \\ -\frac{21}{62} & -\frac{3}{62} & \frac{5}{31} & \frac{11}{31} \\ \frac{15}{62} & \frac{11}{62} & -\frac{8}{31} & \frac{1}{31} \end{bmatrix}$$

$$(M^{-1})^T = \begin{bmatrix} \frac{23}{62} & -\frac{3}{62} & -\frac{21}{62} & \frac{15}{62} \\ \frac{21}{62} & -\frac{27}{62} & -\frac{3}{62} & \frac{11}{62} \\ -\frac{4}{31} & \frac{14}{31} & \frac{5}{31} & -\frac{8}{31} \\ -\frac{15}{31} & \frac{6}{31} & \frac{11}{31} & \frac{1}{31} \end{bmatrix}.$$

Karena semua perhitungan dipengaruhi oleh aritmatika modulo, maka nilai invers pada matriks akan disederhanakan menggunakan aritmatika modulo. Karena pada matriks di atas $det < -1$ maka proses dilanjutkan dengan menghitung invers pada aritmatika modulo sebagai berikut :

$aa^{-1} = a^{-1}a = 1(mod\ m)$

$-62 \times -62^{-1} = 1(mod\ 29)$

$1 = 7(-62) mod\ 29$

$1 = -434\ mod\ 29.$

Maka invers matriks yang sesuai dengan perhitungan invers modulo di atas yaitu :

$$M^{-1} = 7\begin{bmatrix} k_{11} & k_{21} & k_{31} & k_{41} \\ k_{12} & k_{22} & k_{32} & k_{42} \\ k_{13} & k_{23} & k_{33} & k_{43} \\ k_{14} & k_{24} & k_{34} & k_{44} \end{bmatrix} mod\ 29$$

Jadi, $$M^{-1} = 7\begin{bmatrix} -23 & -21 & 8 & 30 \\ 3 & 27 & 28 & 12 \\ 21 & 3 & -10 & -22 \\ -15 & -11 & 16 & -2 \end{bmatrix} mod\ 29$$

$$M^{-1} = \begin{bmatrix} -161 & -147 & 56 & 210 \\ 21 & 189 & 196 & 84 \\ 147 & 21 & -70 & -154 \\ -105 & -77 & 112 & -14 \end{bmatrix} mod\ 29$$

$$M^{-1} = \begin{bmatrix} 13 & 27 & 27 & 7 \\ 21 & 15 & 7 & 3 \\ 2 & 21 & 17 & 20 \\ 11 & 10 & 25 & 15 \end{bmatrix}$$

$$(M^{-1})^T = \begin{bmatrix} 13 & 21 & 2 & 11 \\ 27 & 15 & 21 & 10 \\ 27 & 7 & 17 & 25 \\ 7 & 3 & 20 & 15 \end{bmatrix}.$$

4. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks M diambil dari matriks A. Mengganti semua elemen lain dengan nol. Matriks disebut G.

$$G = \begin{bmatrix} 13 & 21 & 2 & 11 & 0 \\ 27 & 15 & 21 & 10 & 0 \\ 27 & 7 & 17 & 25 & 0 \\ 7 & 3 & 20 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

5. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi

$$G^T = g = \begin{bmatrix} 13 & 27 & 27 & 7 & 0 \\ 21 & 15 & 7 & 3 & 0 \\ 2 & 21 & 17 & 20 & 0 \\ 11 & 10 & 25 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

bukti bahwa matriks di atas adalah matriks invers tergeneralisasi yaitu memenuhi sifat :

c) $gAg = g$.

d) $AgA = A$.

Bukti :

$$g = \begin{bmatrix} 13 & 27 & 27 & 7 & 0 \\ 21 & 15 & 7 & 3 & 0 \\ 2 & 21 & 17 & 20 & 0 \\ 11 & 10 & 25 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}$$

$$Ag = \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} 13 & 27 & 27 & 7 & 0 \\ 21 & 15 & 7 & 3 & 0 \\ 2 & 21 & 17 & 20 & 0 \\ 11 & 10 & 25 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 88 & 87 & 116 & 58 & 0 \\ 58 & 175 & 174 & 116 & 0 \\ 87 & 174 & 146 & 87 & 0 \\ 58 & 87 & 116 & 88 & 0 \\ 58 & 175 & 174 & 116 & 0 \end{bmatrix} mod\ 29$$

$$AgA = \begin{bmatrix} 88 & 87 & 116 & 58 & 0 \\ 58 & 175 & 174 & 116 & 0 \\ 87 & 174 & 146 & 87 & 0 \\ 58 & 87 & 116 & 88 & 0 \\ 58 & 175 & 174 & 116 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 697 & 466 & 812 & 525 & 1046 \\ 1105 & 580 & 1454 & 697 & 1626 \\ 1047 & 553 & 1308 & 696 & 1454 \\ 667 & 436 & 872 & 525 & 1106 \\ 1105 & 580 & 1454 & 697 & 1626 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 1 & 2 & 0 & 3 & 2 \\ 3 & 0 & 4 & 1 & 2 \\ 3 & 2 & 3 & 0 & 4 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 0 & 4 & 1 & 2 \end{bmatrix}.$$

■

Langkah 3 : Prosedur Pertukaran Kunci Diffie-Hellman

Mengaplikasikan semua kesepakatan yang telah dibuat dengan melakukan proses pada protokol pertukaran kunci Diffie-Hellman sebagai berikut :

1. Pengguna pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada pengguna kedua sebagai berikut :

   $X = g^x \ mod \ n.$

   Bilangan bulat yang dipilih oleh pengguna pertama hanya pengguna pertama yang tahu. Misalkan pengguna pertama memilih bilangan bulat $x = 7$, maka perhitungan X yang diperoleh yaitu :

   $$X = \begin{bmatrix} 13 & 27 & 27 & 7 & 0 \\ 21 & 15 & 7 & 3 & 0 \\ 2 & 21 & 17 & 20 & 0 \\ 11 & 10 & 25 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}^7 \ mod\ 29$$

   Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13*. Maka diperoleh matriks X yaitu :

   $$X = \begin{bmatrix} 11 & 22 & 3 & 1 & 0 \\ 16 & 22 & 24 & 16 & 0 \\ 17 & 13 & 20 & 17 & 0 \\ 24 & 7 & 16 & 18 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

   Proses selengkapnya dapat dilihat pada lampiran A.

2. Pengguna kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada pengguna pertama:

   $Y = g^y \ mod \ n.$

   Sama halnya dengan pengguna pertama, bilangan bulat yang dipilih oleh pengguna kedua hanya pengguna kedua yang tahu. Misalkan pengguna kedua memilih bilangan bulat $y = 45$, maka perhitungan Y yang diperoleh yaitu :

$$Y = \begin{bmatrix} 13 & 27 & 27 & 7 & 0 \\ 21 & 15 & 7 & 3 & 0 \\ 2 & 21 & 17 & 20 & 0 \\ 11 & 10 & 25 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{45} \quad mod\ 29$$

Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13*. Maka diperoleh matriks Y yaitu :

$$Y = \begin{bmatrix} 14 & 0 & 27 & 9 & 0 \\ 20 & 7 & 27 & 20 & 0 \\ 19 & 10 & 1 & 4 & 0 \\ 4 & 16 & 6 & 26 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran B.

3. Pengguna pertama menghitung

$K = Y^x \ mod\ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K = \begin{bmatrix} 14 & 0 & 27 & 9 & 0 \\ 20 & 7 & 27 & 20 & 0 \\ 19 & 10 & 1 & 4 & 0 \\ 4 & 16 & 6 & 26 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}^7 mod\ 29$$

$$= \begin{bmatrix} 23 & 5 & 10 & 26 & 0 \\ 2 & 27 & 19 & 3 & 0 \\ 24 & 12 & 9 & 10 & 0 \\ 4 & 11 & 18 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran C.

4. Pengguna kedua menghitung

$K' = X^y \ mod\ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K' = \begin{bmatrix} 11 & 22 & 3 & 1 & 0 \\ 16 & 22 & 24 & 16 & 0 \\ 17 & 13 & 20 & 17 & 0 \\ 24 & 7 & 16 & 18 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{27} \ mod\ 29$$

$$= \begin{bmatrix} 23 & 5 & 10 & 26 & 0 \\ 2 & 27 & 19 & 3 & 0 \\ 24 & 12 & 9 & 10 & 0 \\ 4 & 11 & 18 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran D.

Terlihat bahwa perhitungan dilakukan dengan benar. Hal ini ditunjukkan dengan $K = K' = \begin{bmatrix} 23 & 5 & 10 & 26 & 0 \\ 2 & 27 & 19 & 3 & 0 \\ 24 & 12 & 9 & 10 & 0 \\ 4 & 11 & 18 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Jadi, dari semua perhitungan diperoleh K dan K' yang merupakan kunci bersama yang dimiliki oleh pengguna pertama dan pengguna kedua. Kunci ini merupakan kunci rahasia bagi kedua pengguna. Sehingga, kedua pengguna tersebut dapat melakukan pengiriman pesan dalam bentuk *chipper* yang hanya dapat dibaca oleh kedua pengguna yang saling mempunyai kunci yang sama.

Contoh 4.3 (Matriks M juga mempunyai determinan sama dengan nol)

Diberikan kesepakatan sebagai berikut :

1. Ordo matriks yaitu ordo 5.
2. Elemen matriks $A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$.
3. Letak *rank* matriks yaitu kiri atas.
4. Operator modulo yang digunakan yaitu $mod = 29$.

Penyelesaian :

Langkah 1 : Identifikasi Matriks

Identifikasi matriks ini menggunakan program *maple 13*.

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$$

$\det A = 0$.

Identifikasi matriks dari kesepakatan tersebut menghasilkan determinan sama dengan nol (0) yang berarti syarat untuk matriks invers tergeneralisasi terpenuhi. Maka proses dapat dilanjutkan pada langkah selanjutnya.

Langkah 2 : Matriks Invers Tergeneralisasi.

1. Menghitung *rank* matriks dengan menggunakan OBE.

   Diketahui matriks $A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$

   berikut perhitungan dengan menggunakan OBE.

   a. Mengurangkan baris ke-2 dengan baris ke-1

   $$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} b2 - b1$$

   $$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$$

   b. Mengurangkan baris ke-3 dengan $\frac{6}{5}$ baris ke-1

   $$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} b3 - \frac{6}{5} b1$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$$

c. Mengurangkan baris ke-4 dengan $\frac{6}{5}$ kali baris ke-1

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} b4 - \frac{6}{5} b1$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$$

d. Mengurangkan baris ke-5 dengan baris ke-1

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} b5 - b1$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix}$$

e. Mengurangkan baris ke-3 dengan $\frac{13}{5}$ kali baris ke-2

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & -2.6 & -0{,}4 & 3 & -1 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix} b3 - \frac{13}{5} b2$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix}$$

f. Mengurangkan baris ke-4 dengan $\frac{2}{5}$ kali baris ke-2

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0{,}4 & -1{,}4 & 1 & 0 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix} b4 - \frac{2}{5}b2$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0 & -2{,}2 & 2{,}2 & 0{,}4 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix}$$

g. Mengurangkan baris ke-5 dengan baris ke-2

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0 & -2{,}2 & 2{,}2 & 0{,}4 \\ 0 & -1 & -2 & 3 & 1 \end{bmatrix} b5 - b2$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0 & -2{,}2 & 2{,}2 & 0{,}4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

h. Mengurangkan baris ke-5 dengan baris ke-2

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0 & -2{,}2 & 2{,}2 & 0{,}4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} b4 - \frac{11}{24}b3$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 0 & -1 & -2 & 3 & 1 \\ 0 & 0 & 4{,}8 & -4{,}8 & -3{,}6 \\ 0 & 0 & 0 & 0 & -1{,}25 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hasil Perhitungan diatas dengan menggunakan OBE diperoleh *rank* matriks $A = r(A) = 4$. Maka ordo untuk matriks M adalah matriks 4×4.

2. Menghitung determinan matriks M yang merupakan cerminan matriks non-singular.

Matriks M merupakan matriks minor dari matriks A yang letak pengambilannya merupakan suatu kesepakatan. Berikut matriks dari kesepakatan tersebut:

$$M = \begin{bmatrix} 5 & 3 & 2 & 0 \\ 5 & 2 & 0 & 3 \\ 6 & 1 & 2 & 3 \\ 6 & 4 & 1 & 1 \end{bmatrix}.$$

Pembuktian bahwa matriks ini merupakan cerminan matriks non-singular yaitu menggunakan metode kofaktor:

$$\det M = (-1)^{1+1}(5)\begin{vmatrix} 5 & 3 & 2 & 0 \\ 5 & 2 & 0 & 3 \\ 6 & 1 & 2 & 3 \\ 6 & 4 & 1 & 1 \end{vmatrix} + (-1)^{1+2}(3)\begin{vmatrix} 5 & 3 & 2 & 0 \\ 5 & 2 & 0 & 3 \\ 6 & 1 & 2 & 3 \\ 6 & 4 & 1 & 1 \end{vmatrix}$$

$$+(-1)^{1+3}(2)\begin{vmatrix} 5 & 3 & 2 & 0 \\ 5 & 2 & 0 & 3 \\ 6 & 1 & 2 & 3 \\ 6 & 4 & 1 & 1 \end{vmatrix} + (-1)^{1+4}(0)\begin{vmatrix} 5 & 3 & 2 & 0 \\ 5 & 2 & 0 & 3 \\ 6 & 1 & 2 & 3 \\ 6 & 4 & 1 & 1 \end{vmatrix}$$

$$= \left(5(-1)^{1+1}(2)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix} + 5(-1)^{1+2}(0)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix} + \right.$$

$$\left. 5(-1)^{1+3}(3)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix}\right) - \left(3(-1)^{1+1}(5)\begin{vmatrix} 5 & 0 & 3 \\ 6 & 2 & 3 \\ 6 & 1 & 1 \end{vmatrix} + \right.$$

$$\left. 3(-1)^{1+2}(0)\begin{vmatrix} 5 & 0 & 3 \\ 6 & 2 & 3 \\ 6 & 1 & 1 \end{vmatrix} + 3(-1)^{1+3}(3)\begin{vmatrix} 5 & 0 & 3 \\ 6 & 2 & 3 \\ 6 & 1 & 1 \end{vmatrix}\right) +$$

$$\left(2(-1)^{1+1}(5)\begin{vmatrix} 5 & 2 & 3 \\ 6 & 1 & 3 \\ 6 & 4 & 1 \end{vmatrix} + 2(-1)^{1+2}(2)\begin{vmatrix} 5 & 2 & 3 \\ 6 & 1 & 3 \\ 6 & 4 & 1 \end{vmatrix}\right.$$

$$\left. 2(-1)^{1+3}(3)\begin{vmatrix} 5 & 2 & 3 \\ 6 & 1 & 3 \\ 6 & 4 & 1 \end{vmatrix}\right)$$

$$= (-10 + 0 - 105) - (-15 + 0 - 54) + (-110 - (-48) + 108)$$

$$= 0.$$

Karena hasil dari kesepakatan letak *rank* yang digunakan juga menghasilkan matriks singular, maka terjadi perubahan kesepakatan letak *rank*. Letak *rank* untuk kesepakatan kedua adalah kanan atas. Maka diperoleh matriks :

$$M = \begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix}$$

Selanjutnya dilakukan kembali pembuktian bahwa matriks ini merupakan cerminan matriks non-singular yaitu menggunakan metode kofaktor

$$\det M = (-1)^{1+1}(3)\begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix} + (-1)^{1+2}(2)\begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix}$$

$$+(-1)^{1+3}(0)\begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix} + (-1)^{1+4}(5)\begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix}$$

$$= \left(3(-1)^{1+1}(0)\begin{vmatrix} 0 & 3 & 6 \\ 2 & 3 & 5 \\ 1 & 1 & 6 \end{vmatrix} + 3(-1)^{1+2}(3)\begin{vmatrix} 0 & 3 & 6 \\ 2 & 3 & 5 \\ 1 & 1 & 6 \end{vmatrix} + \right.$$

$$\left. 3(-1)^{1+3}(6)\begin{vmatrix} 0 & 3 & 6 \\ 2 & 3 & 5 \\ 1 & 1 & 6 \end{vmatrix}\right) - \left(2(-1)^{1+1}(2)\begin{vmatrix} 2 & 3 & 6 \\ 1 & 3 & 5 \\ 4 & 1 & 6 \end{vmatrix} + \right.$$

$$\left. 2(-1)^{1+2}(3)\begin{vmatrix} 2 & 3 & 6 \\ 1 & 3 & 5 \\ 4 & 1 & 6 \end{vmatrix} + 2(-1)^{1+3}(6)\begin{vmatrix} 2 & 3 & 6 \\ 1 & 3 & 5 \\ 4 & 1 & 6 \end{vmatrix}\right) -$$

$$\left(5(-1)^{1+1}(2)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix} + 5(-1)^{1+2}(0)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix} + \right.$$

$$\left. 5(-1)^{1+3}(3)\begin{vmatrix} 2 & 0 & 3 \\ 1 & 2 & 3 \\ 4 & 1 & 1 \end{vmatrix}\right)$$

$$= (0 - 63 - 18) - (52 + 84 - 132) - (-10 - 0 - 105)$$

$$= 30.$$

Terbukti bahwa determinan matriks di atas $\neq 0$, maka proses dapat dilanjutkan pada langkah selanjutnya.

3. Invers matriks M, kemudian tansposkan.

   Invers dan transpos matriks M Menggunakan program *maple 13* yang hasilnya yaitu :

$$M = \begin{bmatrix} 3 & 2 & 0 & 5 \\ 2 & 0 & 3 & 6 \\ 1 & 2 & 3 & 5 \\ 4 & 1 & 1 & 6 \end{bmatrix}$$

$$M^{-1} = \frac{1}{\det M} adj\ M$$

$$= \frac{1}{30} \begin{bmatrix} -27 & -21 & 9 & 36 \\ -2 & -16 & 14 & 6 \\ -28 & -14 & 16 & 24 \\ 23 & 19 & -11 & -24 \end{bmatrix}$$

$$= \begin{bmatrix} -\frac{9}{10} & -\frac{7}{10} & \frac{3}{10} & \frac{6}{5} \\ -\frac{1}{15} & -\frac{8}{15} & \frac{7}{15} & \frac{1}{5} \\ -\frac{14}{15} & -\frac{7}{15} & \frac{8}{15} & \frac{4}{5} \\ \frac{23}{30} & \frac{19}{30} & -\frac{11}{30} & -\frac{4}{5} \end{bmatrix}$$

$$(M^{-1})^T = \begin{bmatrix} \frac{23}{62} & -\frac{1}{15} & -\frac{14}{15} & \frac{23}{30} \\ -\frac{7}{10} & -\frac{8}{15} & -\frac{7}{15} & \frac{19}{30} \\ \frac{3}{10} & \frac{7}{15} & \frac{8}{15} & -\frac{11}{30} \\ \frac{6}{5} & \frac{1}{5} & \frac{4}{5} & -\frac{4}{5} \end{bmatrix}.$$

Karena semua perhitungan dipengaruhi oleh aritmatika modulo, maka nilai invers pada matriks akan disederhanakan menggunakan aritmatika modulo. Karena pada matriks di atas $det > 1$ maka proses dilanjutkan dengan menghitung invers pada aritmatika modulo sebagai berikut :

$$aa^{-1} = a^{-1}a = 1(mod\ m)$$

$$30 \times 30^{-1} = 1(mod\ 29)$$

$$1 = 1(30) mod\ 29$$

$$1 = 30\ mod\ 29.$$

Maka invers matriks yang sesuai dengan perhitungan invers modulo di atas yaitu :

$$M^{-1} = 1 \begin{bmatrix} k_{11} & k_{21} & k_{31} & k_{41} \\ k_{12} & k_{22} & k_{32} & k_{42} \\ k_{13} & k_{23} & k_{33} & k_{43} \\ k_{14} & k_{24} & k_{34} & k_{44} \end{bmatrix} mod\ 29$$

Jadi $M^{-1} = 1 \begin{bmatrix} -27 & -21 & 9 & 36 \\ -2 & -16 & 14 & 6 \\ -28 & -14 & 16 & 24 \\ 23 & 19 & -11 & -24 \end{bmatrix} mod\ 29$

$$M^{-1} = \begin{bmatrix} -27 & -21 & 9 & 36 \\ -2 & -16 & 14 & 6 \\ -28 & -14 & 16 & 24 \\ 23 & 19 & -11 & -24 \end{bmatrix} mod\ 29$$

$$M^{-1} = \begin{bmatrix} 2 & 8 & 9 & 7 \\ 27 & 13 & 14 & 6 \\ 1 & 15 & 16 & 24 \\ 23 & 19 & 18 & 5 \end{bmatrix}$$

$$(M^{-1})^T = \begin{bmatrix} 2 & 27 & 1 & 23 \\ 8 & 13 & 15 & 19 \\ 9 & 14 & 16 & 18 \\ 7 & 6 & 24 & 5 \end{bmatrix}.$$

4. Letakkan nilai invers matriks M yang telah ditransposkan pada tempat awal ketika nilai matriks M diambil dari matriks A. Mengganti semua elemen lain dengan nol. Matriks disebut G.

$$G = \begin{bmatrix} 0 & 2 & 27 & 1 & 23 \\ 0 & 8 & 13 & 15 & 19 \\ 0 & 9 & 14 & 16 & 18 \\ 0 & 7 & 6 & 24 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

a. Transpos matriks. Hasil dari transpos adalah matriks invers tergeneralisasi.

$$G^T = g = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 9 & 7 & 0 \\ 27 & 13 & 14 & 6 & 0 \\ 1 & 15 & 16 & 24 & 0 \\ 23 & 19 & 18 & 5 & 0 \end{bmatrix}.$$

bukti bahwa matriks di atas adalah matriks invers tergeneralisasi yaitu memenuhi sifat :

e) $gAg = g$.

f) $AgA = A$.

Bukti :

$$g = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 9 & 7 & 0 \\ 27 & 13 & 14 & 6 & 0 \\ 1 & 15 & 16 & 24 & 0 \\ 23 & 19 & 18 & 5 & 0 \end{bmatrix}$$

$$A = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}$$

$$Ag = \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 9 & 7 & 0 \\ 27 & 13 & 14 & 6 & 0 \\ 1 & 15 & 16 & 24 & 0 \\ 23 & 19 & 18 & 5 & 0 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 175 & 145 & 145 & 58 & 0 \\ 145 & 175 & 174 & 116 & 0 \\ 174 & 174 & 175 & 116 & 0 \\ 174 & 174 & 174 & 88 & 0 \\ 145 & 175 & 174 & 116 & 0 \end{bmatrix} mod\ 29$$

$$AgA = \begin{bmatrix} 175 & 145 & 145 & 58 & 0 \\ 145 & 175 & 174 & 116 & 0 \\ 174 & 174 & 175 & 116 & 0 \\ 174 & 174 & 174 & 88 & 0 \\ 145 & 175 & 174 & 116 & 0 \end{bmatrix} \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 2818 & 1192 & 698 & 928 & 2818 \\ 3340 & 1423 & 754 & 1163 & 3341 \\ 3486 & 1509 & 814 & 1163 & 3485 \\ 3312 & 1396 & 784 & 1132 & 3312 \\ 3340 & 1423 & 754 & 1163 & 3341 \end{bmatrix} mod\ 29$$

$$= \begin{bmatrix} 5 & 3 & 2 & 0 & 5 \\ 5 & 2 & 0 & 3 & 6 \\ 6 & 1 & 2 & 3 & 5 \\ 6 & 4 & 1 & 1 & 6 \\ 5 & 2 & 0 & 3 & 6 \end{bmatrix}.$$

■

Langkah 3 : Prosedur Pertukaran Kunci Diffie-Hellman

Mengaplikasikan semua kesepakatan yang telah dibuat dengan melakukan proses pada protokol pertukaran kunci Diffie-Hellman sebagai berikut :

1. Pengguna pertama memilih bilangan bulat acak yang besar x dan mengirim hasil perhitungan berikut kepada pengguna kedua sebagai berikut :

   $X = g^x \ mod\ n.$

   Bilangan bulat yang dipilih oleh pengguna pertama hanya pengguna pertama yang tahu. Misalkan pengguna pertama memilih bilangan bulat $x = 13$, maka perhitungan X yang diperoleh yaitu :

$$X = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 9 & 7 & 0 \\ 27 & 13 & 14 & 6 & 0 \\ 1 & 15 & 16 & 24 & 0 \\ 23 & 19 & 18 & 5 & 0 \end{bmatrix}^{13} \ mod\ 29$$

   Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13*. Maka diperoleh matriks X yaitu :

$$X = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 10 & 10 & 15 & 3 & 0 \\ 22 & 27 & 0 & 3 & 0 \\ 9 & 12 & 16 & 1 & 0 \\ 20 & 18 & 20 & 26 & 0 \end{bmatrix}.$$

   Proses selengkapnya dapat dilihat pada lampiran A.

2. Pengguna kedua memilih bilangan bulat acak yang besar y dan mengirim hasil perhitungan berikut kepada pengguna pertama:

   $Y = g^y \ mod\ n.$

   Sama halnya dengan pengguna pertama, bilangan bulat yang dipilih oleh pengguna kedua hanya pengguna kedua yang tahu. Misalkan pengguna kedua memilih bilangan bulat $y = 23$, maka perhitungan Y yang diperoleh yaitu :

$$Y = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 9 & 7 & 0 \\ 27 & 13 & 14 & 6 & 0 \\ 1 & 15 & 16 & 24 & 0 \\ 23 & 19 & 18 & 5 & 0 \end{bmatrix}^{23} \ mod\ 29$$

Karena menggunakan perkalian matriks dengan pangkat yang besar maka penyelesaian ini menggunakan program *maple 13*. Maka diperoleh matriks Y yaitu :

$$Y = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 5 & 25 & 20 & 17 & 0 \\ 4 & 28 & 3 & 0 & 0 \\ 22 & 21 & 18 & 23 & 0 \\ 7 & 26 & 10 & 13 & 0 \end{bmatrix}.$$

Proses selengkapnya dapat dilihat pada lampiran B.

3. Pengguna pertama menghitung

$K = Y^x \ mod \ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 5 & 25 & 20 & 17 & 0 \\ 4 & 28 & 3 & 0 & 0 \\ 22 & 21 & 18 & 23 & 0 \\ 7 & 26 & 10 & 13 & 0 \end{bmatrix}^{13} \ mod \ 29$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 22 & 19 & 24 & 20 & 0 \\ 7 & 16 & 18 & 26 & 0 \\ 17 & 13 & 22 & 27 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Proses selengkapnya dapat dilihat pada lampiran C.

5. Pengguna kedua menghitung

$K' = X^y \ mod \ n.$

Proses yang akan digunakan menggunakan program *maple 13*, karena sulitnya untuk menghitung matrik berpangkat > 2. Berikut ditampilkan hasil perhitungan :

$$K' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 10 & 10 & 15 & 3 & 0 \\ 22 & 27 & 0 & 3 & 0 \\ 9 & 12 & 16 & 1 & 0 \\ 20 & 18 & 20 & 26 & 0 \end{bmatrix}^{23} \ mod \ 29$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 22 & 19 & 24 & 20 & 0 \\ 7 & 16 & 18 & 26 & 0 \\ 17 & 13 & 22 & 27 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Proses selengkapnya dapat dilihat pada lampiran D.

Terlihat bahwa perhitungan dilakukan dengan benar. Hal ini ditunjukkan dengan $K = K' = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 22 & 19 & 24 & 20 & 0 \\ 7 & 16 & 18 & 26 & 0 \\ 17 & 13 & 22 & 27 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$. Jadi, dari semua perhitungan diperoleh K dan K' yang merupakan kunci bersama yang dimiliki oleh pengguna pertama dan pengguna kedua. Kunci ini merupakan kunci rahasia bagi kedua pengguna. Sehingga, kedua pengguna tersebut dapat melakukan pengiriman pesan dalam bentuk *chipper* yang hanya dapat dibaca oleh kedua pengguna yang saling mempunyai kunci yang sama.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan pada bab IV, diperoleh hasil penelitian yaitu pertukaran kunci dengan algoritma Diffie-Hellman dapat menggunakan jenis matriks invers tergeneralisasi dengan langkah-langkah sebagai berikut :

a. Melakukan identifikasi matriks

b. Memperoleh matriks invers tergeneralisasi dengan ketentuan yaitu :

   1. Jika matriks M nilai $\det(M) = 1$ atau $\det(M) = -1$, maka proses dilanjutkan pada langkah pertukaran kunci.
   2. Jika matriks M nilai $\det(M) < -1$ atau $\det(M) > 1$, maka dilakukan pencarian dengan menggunakan invers aritmatika modulo kemudian dilanjutkan pada langkah pertukaran kunci.
   3. Jika kesepakatan letak *rank* matriks yang disebut matriks M juga mempunyai nilai determinan sama dengan nol, maka kesepakatan untuk letak *rank* akan diubah.

c. Melakukan prosedur pertukaran kunci dengan Diffie-Hellman.

Jika langkah-langkah dan perhitungan dilakukan dengan benar, maka kunci yang dihasilkan akan sama bagi pelaku pertukaran kunci. Hal ini ditunjukkan dengan $K = K' = \begin{bmatrix} 18 & 6 & 6 & 0 \\ 14 & 11 & 12 & 0 \\ 1 & 8 & 12 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ pada contoh 4.1. Kunci yang dihasilkan berupa sebuah matriks yang telah dioperasikan pada langkah-langkah yang ada pada algoritma Diffie-Hellman. Kunci ini merupakan kunci rahasia bagi kedua pengguna. Sehingga, kedua pengguna tersebut dapat melakukan pengiriman pesan dalam bentuk *chipper* yang hanya dapat dibaca oleh kedua pengguna yang saling mempunyai kunci yang sama.

5.2 Saran

Tugas akhir ini, penulis menggunakan matriks invers tergeneralisasi pada algoritma pertukaran kunci Diffie-Hellman, diharapkan bagi pembaca yang berminat dapat menggunakan jenis matriks lain untuk memperoleh kunci pada algoritma Diffie-Hellman.

DAFTAR PUSTAKA

Anton, Howard. *Aljabar Linear Elementer*. Jakarta : Erlangga. 1988.

Anton, Howard dan Rorres. *Penerapan Aljabar Linear*. Jakarta: Erlangga. 1988.

H.S, Suryadi. *Pengantar Aljabar Linear Dan Geometri Analitik*. Jakarta : Gunadarma 1995.

Kurniawan, Yusuf. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung : Informatika Bandung. 2004.

Kromodimoeljo, Sentot. *Teori dan Aplikasi Kriptografi*. Jakarta : SPK IT Consulting. 2009.

Menzes,A.J,Oorcshot,P.C dan Vanstone,S.A. *Handbookof Applied Chriptographo.* USA: CRC Press, Inc. 1997.

Murtiyasa, B. "Aplikasi Matriks Invers Tergeneralisasi pada Kriptografi" dalam *Jurnal Penelitian Sain dan Teknologi Vol. 1 Nomor 2 Februari 2001. Hal. 82-90*. Surakarta: Lembaga Penelitian UMS. 2001.

Munir, Rinaldi. *Kriptografi*. Cetakan Pertama. Bandung : Informatika Bandung. 2006.

Munir, Rinaldi. *Matematika Diskrit.* Edisi Ketiga. Bandung : Informatika Bandung. 2007.

Oladejo, Nathaniel dan Apio, Dominic. "On the Generalisized Inverse of a Matrix". *EuroJournals Publishing*, Inc. 2010.

Rao, C.R. dan Mitra, S.K. *Generalized Inverse Matrices dan its Applications*. New York : John Wiley & Sons, Inc. 1971.

Rianto, Muhamad Zaki. *"Aplikasi Aljabar Pada Kriptografi dan Keamanan Informasi"*. Makalah

T. Sutojo, dkk. *Teori dan Aplikasi Aljabar Linear & Matriks.* Yogyakarta: Penerbit Andi. 2010.